ČESKÁ TECHNICKÁ NORMA

ICS 35.240.99 **Září 2016**

Elektronické podpisy a infrastruktury (ESI) – Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty – Část 1: Obecné požadavky

ČSN
ETSI EN 319 411-1
V1.1.1
87 4007

Electronic Signatures and Infrastructures (ESI) – Policy and security requirements for Trust Service Providers issuing
certificates –
Part 1: General requirements

Tato norma přejímá anglickou verzi evropské normy ETSI EN 319 411-1 V1.1.1:2016. Má stejný status jako oficiální verze.

This standard implements the English version of the European Standard ETSI EN 319 411-1 V1.1.1:2016. It has the same status as the official version.

Anotace obsahu

Tento dokument specifikuje obecně použitelné požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb (TSP) vydávající certifikáty veřejného klíče, včetně certifikátů důvěryhodných webových stránek.

Požadavky politiky a bezpečnosti jsou definovány z hlediska požadavků na správu vydávání, udržování a životnosti certifikátů. Tyto požadavky politiky a bezpečnosti podporují šest referenčních certifikačních politik definovaných v kapitole 5.

Rámec pro definování požadavků politiky pro TSP vydávající certifikáty ve specifickém kontextu, kde platí konkrétní požadavky, je definován v kapitole 7.

Tento dokument pokrývá požadavky na hierarchie CA (certifikační autorita), ale toto je omezeno na podporu politik specifikovaných v této normě. Neobsahuje požadavky na hlavní CA a mezilehlé CA pro jiné účely.

Tento dokument je použitelný pro:

- obecné požadavky na certifikaci při podpoře kryptografických mechanismů, včetně digitálních podpisů a pečetí;
- obecné požadavky na certifikační autority vydávající certifikáty TLS/SSL;
- obecné požadavky na použití kryptografie pro autentizaci a šifrování.

Tento dokument nespecifikuje, jak může uvedené požadavky posuzovat nezávislá strana, včetně požadavků na informace, které mají být zpřístupněny těmto nezávislým posuzovatelům, nebo požadavků na tyto posuzovatele.

Tento dokument však v příloze C uvádí kontrolní seznam požadavků politiky specifických pro TSP vydávající certifikáty (vyjádřených v tomto dokumentu) včetně základních požadavků, které jsou nezávislé na typu služby (vyjádřených v ETSI EN 319 401).

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 15408 (části 1 až 3) zavedeny v částech 1 až 3 souboru ČSN ISO/IEC 15408 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT

ETSI EN 319 412-4 dosud nezavedena

ISO/IEC 19790:2012 nezavedena

CA/Browser Forum V1.5.5: Směrnice pro vydávání a management rozšířených validačních certifikátů nezavedeny

CA/Browser Forum V1.3.0: Základní požadavky na vydávání a management veřejně důvěryhodných certifikátů
nezavedeny

ISO/IEC 9594-8/Doporučení ITU-T X.509 nezavedeny

IETF RFC 5280 nezavedena

ETSI EN 319 401 zavedena v ČSN ETSI EN 319 401 V2.1.1 (87 4006) Elektronické podpisy a infrastruktury (ESI) – Obecné požadavky politiky na poskytovatele důvěryhodných služeb podporující elektronické podpisy

ETSI EN 319 412-2 zavedena v ČSN ETSI EN 319 412-2 V2.1.1 (87 4008) Elektronické podpisy a infrastruktury (ESI) – Profily certifikátu – Část 2: Profil certifikátu pro certifikáty vydávané fyzickým osobám

ETSI EN 319 412-3 dosud nezavedena

IETF RFC 6960 nezavedena

FIPS PUB 140-2:2001 nezavedena

ETSI EN 319 403 zavedena v ČSN ETSI EN 319 403 V2.2.2 (87 4010) Elektronické podpisy a infrastruktury (ESI) – Posuzování shody poskytovatelů důvěryhodných služeb – Požadavky na orgány posuzování shody posuzující poskytovatele důvěryhodných služeb

IETF RFC 3647 nezavedena

ISO 19005 (části 1 až 3) nezavedeny

ETSI EN 319 411-2 zavedena v ČSN ETSI EN 319 411-2 V1.1.1 (87 4007) Elektronické podpisy a infrastruktury (ESI) – Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty – Část 2: Požadavky politiky na certifikační autority vydávající kvalifikované certifikáty

ETSI TS 102 042 nezavedena

ISO/IEC 27002:2013 zavedena v ČSN ISO/IEC 27002:2014 (36 9798) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací

ISO/IEC 7498-2/Doporučení ITU-T X.800 nezavedeny

CEN TS 419 261 nezavedena

ETSI TS 119 312 nezavedena

IETF RFC 5246 nezavedena

ETSI TS 119 612 nezavedena

ETSI TS 101 533-1 nezavedena

ETSI EN 319 421 dosud nezavedena

CEN TS 419 221-2 nezavedena

CEN TS 419 221-3 nezavedena

CEN TS 419 221-4 nezavedena

CEN EN 419 221-5 dosud nezavedena

POZNÁMKY

1 Doporučení ITU-T jsou dostupná v Českém metrologickém institutu, Hvožďanská 3, 148 01 Praha 4.

2 Pokud jsou v originálu normy citovány nezaváděné dokumenty ETR, TBR, ES, EG, TS, TR a GSM, jsou dostupné v Informačním centru ÚNMZ.

Souvisící ČSN

ČSN ISO/IEC 15945 (36 9793) Informační technologie – Bezpečnostní techniky – Specifikace služeb TTP na podporu aplikace digitálních podpisů

ČSN ISO/IEC TR 14516 (36 9791) Informační technologie – Bezpečnostní techniky – Směrnice pro používání a řízení služeb důvěryhodných třetích stran

Citované předpisy

Směrnice 1999/93/ES (1999/93/EC) Evropského parlamentu a Rady ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy.

Nařízení (EU) č. 910/2014 Evropského parlamentu a Rady ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení

směrnice 1999/93/ES.

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článcích „Informace o citovaných dokumentech“ a „Souvisící ČSN“ nejnovějšími vydáními, platnými v době schválení této normy. Při používání této normy je třeba vždy použít taková vydání ČSN, která přejímají nejnovější vydání nedatovaných evropských/
mezinárodních norem (včetně všech změn).

Vypracování normy

Zpracovatel: MAREŠKA Praha, IČ 86983555, Ing. Antonín Mareška

Technická normalizační komise: TNK 96 Telekomunikace

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Jan Křivka